HP Integrated Lights-Out security

Technology brief, 7th Edition

Introduction

HP Integrated Lights-Out (iLO) has been widely accepted as the standard for remotely managing the servers in data centers. Most HP ProLiant and Integrity servers include an autonomous iLO management processor on the system board. The iLO processor and firmware let you securely configure and monitor a server locally or remotely over a management network.

This brief addresses a key concern of data center management: security. iLO ensures that your server hardware, firmware, communication interfaces, and deployment capabilities are secure. This brief describes the utilities and services providing access points into iLO or its host system. It also describes how iLO's design protects against access risks.

This brief covers the following versions:

- iLO 3 v1.0 and 1.05
- iLO 2 v1.60
- iLO v1.91

It does not apply to the LO-100 processors in ProLiant 100-series servers.

Protected access to iLO and sensitive information

The iLO user interface includes multi-layer security: authentication, authorization, data integrity, and privacy.

iLO firmware is digitally signed with a private key. Unauthorized code, including anti-virus software, may not be allowed to execute.

Authentication determines who is at the other end of the network connection. iLO authenticates users with 128-bit Secure Socket Layer (SSL) encryption.

Authorization determines whether the user attempting to perform a specific action has the right to do it. Using local accounts, you can define up to 12 separate iLO users and vary their server access rights. Using directory services, you maintain network user accounts and security policies in a central, scalable database that supports thousands of users and system management roles.

Data integrity verifies that no one has altered incoming commands or data. iLO uses digital signatures and trusted Java™ and ActiveX applets (used by the Integrated Remote Console) to verify data integrity.

Privacy refers to confidentiality of sensitive data and transactions. iLO protects privacy through the 128-bit SSL encryption of web pages and the RC4 encryption of remote console and virtual serial port data.

The following sections describe the protection schemes iLO uses to guard against unauthorized access such as phlashing and other attacks.

iLO resistance against phlashing

Phlashing is a permanent denial of service attack (PDOS). PDOS attacks could theoretically take advantage of vulnerabilities during updates of network-based firmware. Rogue firmware installed through a PDOS attack could lead to unauthorized server access or permanent hardware damage.

iLO is not at risk from these vulnerabilities because it offers protection against the following risks:

- Attacks during flash updates – iLO firmware images are digitally signed with a 1024-bit RSA public/private key. The boot block checks the digital signature every time iLO comes out of reset.

iLO 2 and iLO 3 systems check the digital signature before allowing a firmware update to proceed. Remote flashing requires login authentication and authorization, including optional two-factor authentication.

- Unencrypted ports – iLO clearly defines the port encryption status. You can disable access to any non-encrypted ports (such as telnet). Access to iLO requires a password (or an optional trusted certificate for iLO 2), unless you decide to disable the password.

NOTE
iLO 3 does not support telnet.

- Lack of authentication and audit trails – iLO creates a log of SSH authentication failures and successes. SSH-key authentication makes successful brute force attacks even less likely. For additional protection, iLO and iLO 2 offer 2-factor authentication. iLO 3 creates a second session key for remote access.

NOTE
iLO supports only secure shell version 2 (SSH-2).

- Attacks in progress – iLO captures all login activity. It uses a progressive timed delay during unsuccessful login attempts to impede brute force and dictionary attacks.
- Unregulated virtual media access – iLO logs virtual media access so you can trace potential information destroyers.

We address these security topics in more detail later in this technology brief.

Security keys

iLO uses layers of security and industry-standard methods to secure the server. For example, iLO cryptographic keys use a minimum key length of 128 bits and conform to industry standards.

The HP manufacturing process protects sensitive information. We keep no record of initial or default management security keys unless authorized by a "Factory Special" manufacturing process. Manufacturing personnel do not have access to sensitive key or password data. Each server ships with a unique, unpredictable iLO password. This ensures security out-of-the box. If you have specific security requirements, you can order HP servers with pre-configured iLO passwords or use HP deployment utilities to assign your own passwords.

iLO automatically generates new, unique, and site-specific SSL keys when you deploy a server. HP cannot determine these site-specific keys, and iLO does not transmit them to HP.

Physical security

Data center managers are responsible for managing physical access to their facilities. Someone with physical access to a server can alter the iLO setup. We assume that anyone with access to the inside of a server is a super-user or administrator with potential access to the Security Override jumper/switch. You can disable all of iLO's security authorization checks by turning on Security Override. This gives you full access to iLO for the following tasks:

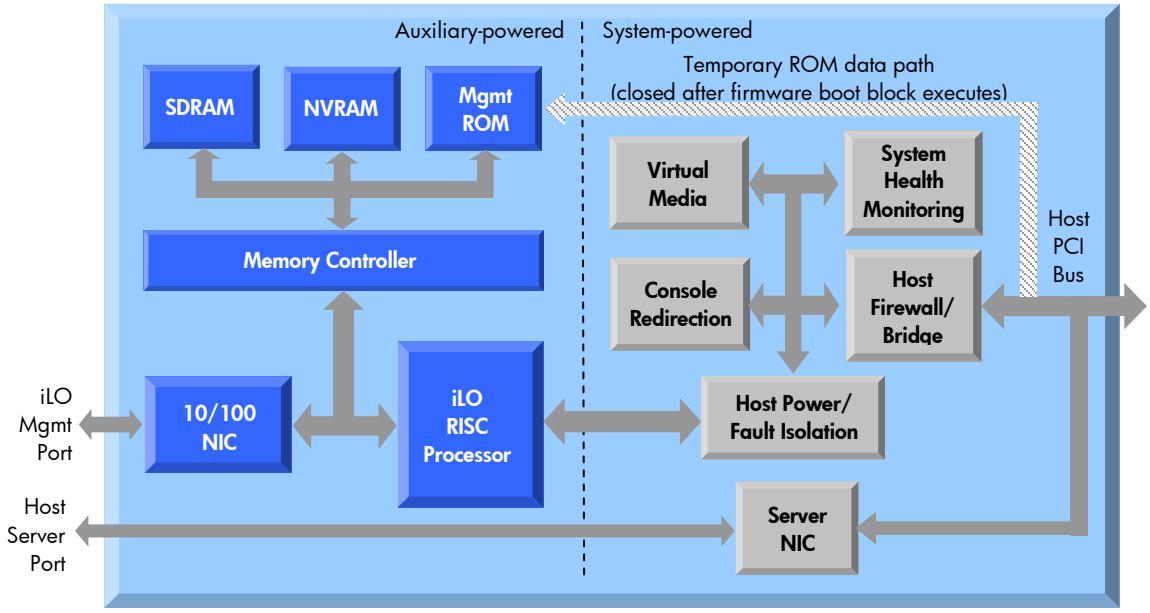
- Reconfigure iLO through ROM-Based Setup (RBSU)

- Reprogram the iLO ROM
- Reprogram the boot block

Security in hardware design

iLO includes a 32-bit, PCI-based ASIC that contains a RISC processor core with separate instruction and data caches, a memory controller, SDRAM, NVRAM, management ROM, and NIC (Figure 1).

Figure 1. Block diagram of iLO processor



Management ROM

The management ROM includes the iLO boot block and the iLO main firmware image. The iLO boot block provides iLO hardware and software setup, locates and validates an executable firmware image, and transfers control to the executable image.

The iLO main image includes an RSA 1024-bit private/public digital signature. HP signs the firmware image with the private key known only to HP. The iLO boot block knows the public key. HP uses this firmware build process to produce the signed image:

1. Compute an SHA 1 (Secure Hash Algorithm) hash over the entire image.
2. Encrypt and sign the SHA1 hash with the RSA private key.
3. Store the encrypted signature in the image header.

The iLO boot block performs the following steps to validate and boot the signed firmware image:

1. Searches memory for a viable image with a recognizable header.
2. Decrypts the signed SHA1 hash using the RSA public key.
3. Computes the SHA1 hash over the entire image.
4. If the two SHA1 hashes match, the image is valid and the boot block passes control to the iLO main image to begin executing.

During a firmware flash process, the iLO boot block performs the following steps to validate a new flash image:

1. The flash routine analyzes the incoming data stream, looking for a viable image.
2. If viable, iLO flashes the image into the Management ROM at the next available address.

Normally, the iLO boot block finds the main image first, and iLO flashes it into the area just past the boot block. The flash process continues until iLO detects no more viable images in the incoming data stream.

iLO and iLO 2 flash the boot block only if the firmware flash happens while you have the iLO Security Override jumper set (disabled). For maximum security, you should not set the Security Override jumper unless you intend to update the boot block. We do not expect that the boot block will require updating, but we provide this mechanism in case you need it. iLO 3 flashes the entire image, including the boot block.

The management ROM uses a temporary ROM data path to the PCI bus on the server (see Figure 1). After the host processor locates iLO and transfers the management ROM code to the host memory, the iLO firmware closes the temporary ROM data path to the host PCI bus. Under normal operating circumstances, there is no chance for the server to flash the management ROM without permission. The host PCI connection remains open only if you access the iLO device in safe mode (by setting the iLO Security Override jumper) or if the iLO firmware does not execute properly. This allows the server to flash the management ROM directly through the host PCI bus if the iLO ROM is corrupted.

Firewall logic

iLO includes firewall and bridge logic to control information flow between the server and the management console (Figure 1). The firewall logic protects against unauthorized access through the server's PCI bus. It shields keys and data stored in memory and firmware.

Memory

iLO contains three classes of memory registers:

- General registers that the server can access through the PCI bus. These PCI registers contain only non-sensitive information. iLO does not secure or try to hide these registers from the server.
- Protected registers where iLO can lock write access. These registers restrict unwanted behavior, such as flashing rogue firmware, but they do not restrict information. They are unlocked in safe mode. Once iLO locks these registers, the server cannot regain control through the PCI bus.
- Secure registers that secure sensitive information such as the configuration data and user passwords. No server application can write to these registers, regardless of the state of the server.

The server can only read the areas of iLO memory that iLO exposes. Applications on the PCI bus can only access the memory that iLO permits, such as the general registers and the protected registers under certain conditions, and cannot change the configuration of any shared memory region.

Non-volatile data storage

The server OS and applications running on the system PCI bus can only read the exposed areas of NVRAM. That includes the integrated management log and server configuration information. An application on the PCI bus cannot change the iLO configuration by means of the exposed NVRAM.

Network and management ports

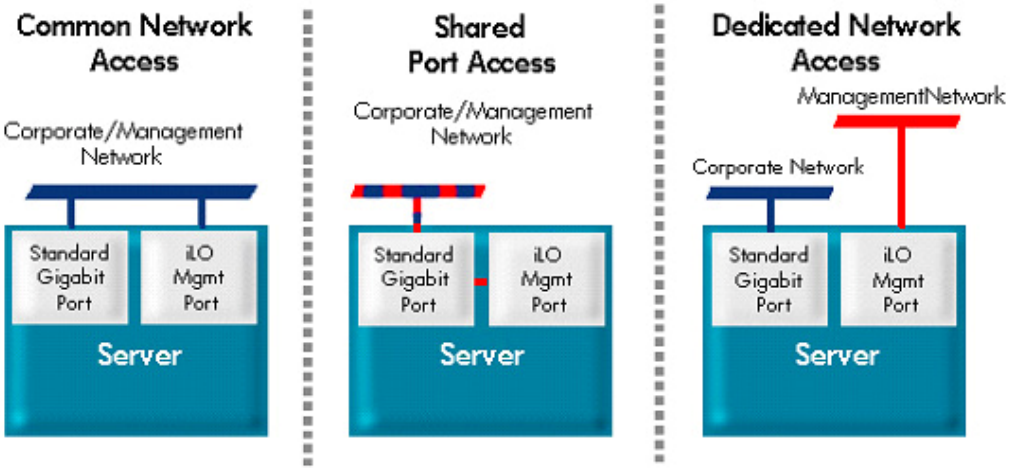
iLO's firewall and bridge logic prevent any connection between the iLO management port and the server Ethernet port (Figure 1). Even by using the shared network port (SNP), iLO cannot bridge traffic between its 10/100 Ethernet port and the server Ethernet port. Therefore, attacks on the server network cannot compromise iLO and vice-versa.

Shared network port

Most G4 and later ProLiant ML and DL servers with iLO support SNP. Consult the server documentation to determine whether your ProLiant server supports SNP. HP does not plan to support SNP on HP BladeSystem server blades.

The SNP lets iLO management traffic use a sideband connection on the server NIC rather than dedicating a second port to iLO management traffic (Figure 2). Although the iLO traffic shares a port with the server OS traffic, both iLO and the server NIC have their own MAC and IP address. This ensures that other devices can independently address iLO. This is an advantage if you want to install and maintain a single network infrastructure for handling both management and productivity traffic.

Figure 2. Traffic paths of shared and dedicated networks



Shared network port with Virtual LAN

Implementing Virtual LAN (VLAN) tags enhances iLO SNP security. When you enable VLAN Tags, the iLO SNP becomes part of a Virtual LAN. The VLAN is a logical network that isolates network traffic to segments. It increases security because established rules keep traffic on one segment from entering another segment. All network devices with the same Virtual LAN tag appear to be on a separate LAN even if they are physically connected to the same LAN. The SNP NIC checks the Ethernet frame for a VLAN ID and compares it against its configured value. If they match, then the SNP strips the frame of the VLAN tag and forwards it to iLO. If they do not match, the SNP forwards the frame to the server. The SNP NIC inserts a VLAN tag into any outgoing Ethernet frames.

This feature is available with iLO v1.80, iLO 2 v1.10 (and later), and iLO 3.

Security techniques used by iLO

Enabling a secure system requires trust that a specific person, computer, or device seeking access has the required authentication and level of authorization. The following sections identify the three essential iLO techniques that you can use to verify trust:

- Authentication and authorization
- Encryption
- Disabling ports and changing port locations

Every function of iLO builds on one or more of these techniques.

Authentication and authorization processes for browser access

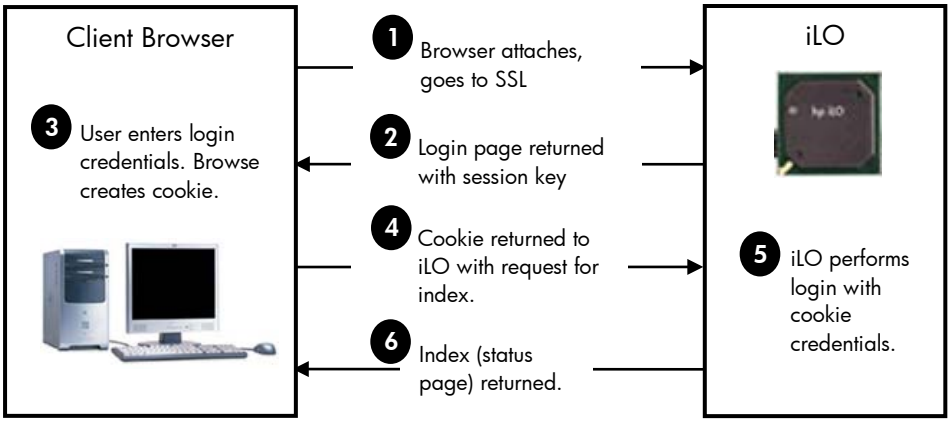
When you access iLO through a browser, iLO authenticates through a local account or through directory services. In either case, iLO re-evaluates privileges every time you make a request to ensure that privileges are still valid. Browser access methods use signed JavaScript or ActiveX controls and do not require an additional login process. The following sections explain how authentication and authorization processes differ between iLO, iLO 2, and iLO 3.

Authentication and authorization with iLO or iLO 2

You can use two-factor authentication to boost iLO security (iLO v1.80 or iLO2 v1.10 and later). This authentication method is more secure than the standard local accounts or directory services methods.

Figure 3 illustrates steps in a successful login/authentication process.

Figure 3. User login process when using a local account (iLO and iLO 2)



LO imposes delays after failed login attempts (Table 1). iLO displays an information page during each delay. The delays will continue until you complete a valid login. This feature assists in defending against possible dictionary attacks against the browser login port. iLO saves a detailed log entry for failed login attempts.

Table 1. iLO response to failed login attempts

Failed attempt	Imposed delay (seconds)
First	5
Second	10
Third	60
Subsequent	60

iLO uses 128-bit SSL encryption and the accompanying digital certificates to encrypt web pages (HTTP data) transmitted across the network. SSL encryption occurs whether the login is through directory services or a local account. SSL encryption ensures that all information and commands issued through the web pages are private. An integral part of SSL is a digital certificate. iLO creates its own self-signed certificate by default. You can also import a certificate from a third party Certificate Authority (CA) or from your organization's internal CA or PKI instead of using the self-signed iLO certificate.

You can use iLO's digital certificate capabilities to prevent malicious attacks (such as Trojan horse attacks) where an impostor appears to be a trusted iLO web server. For example, if someone put a server that emulated iLO onto a corporate network, that server would not have a legitimate iLO certificate. If any user browsed to this emulated iLO device, the browser would flag the lack of a recognized certificate. You can configure the browser to reject a connection to any unrecognized certificates.

Login authentication begins after iLO establishes an SSL connection. iLO sends the user a login page that includes a unique session ID and a random session key. The unique session ID points to a session control block, a memory area where iLO stores all the session information for that user and that session. The session control block eliminates the need to re-authenticate the user credentials for every user request.

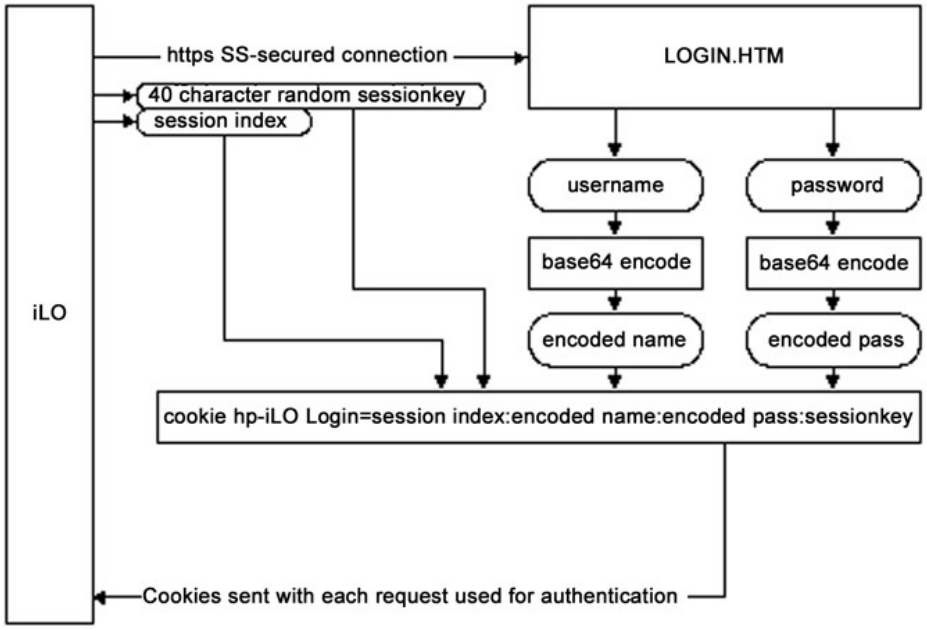
iLO time-stamps the session ID. It is valid only for the length of time defined by the SESSION_TIMEOUT parameter. You can set this parameter to 15, 30, 60, or 120 minutes. iLO 2 firmware after v1.30 supports an Infinite Inactivity Timeout request that extends sessions indefinitely.

The combination of the session ID and the session key prevents another authenticated connection from hijacking a session.

Figure 4 shows how the client browser generates a unique cookie (hp-iLO-Login) for authentication and authorization. The browser encodes both the username and the password using a base-64 hash function and incorporates it into the cookie. The cookie also includes the unique session ID and the random session key sent with the login page.

The cookie links the browser window to the appropriate session in the firmware. The firmware tracks browser logins as separate sessions listed in the Active Sessions section of the iLO Status page.

Figure 4. Flowchart showing how the browser generates the login cookie used for authentication (iLO and iLO 2)



example cookie:

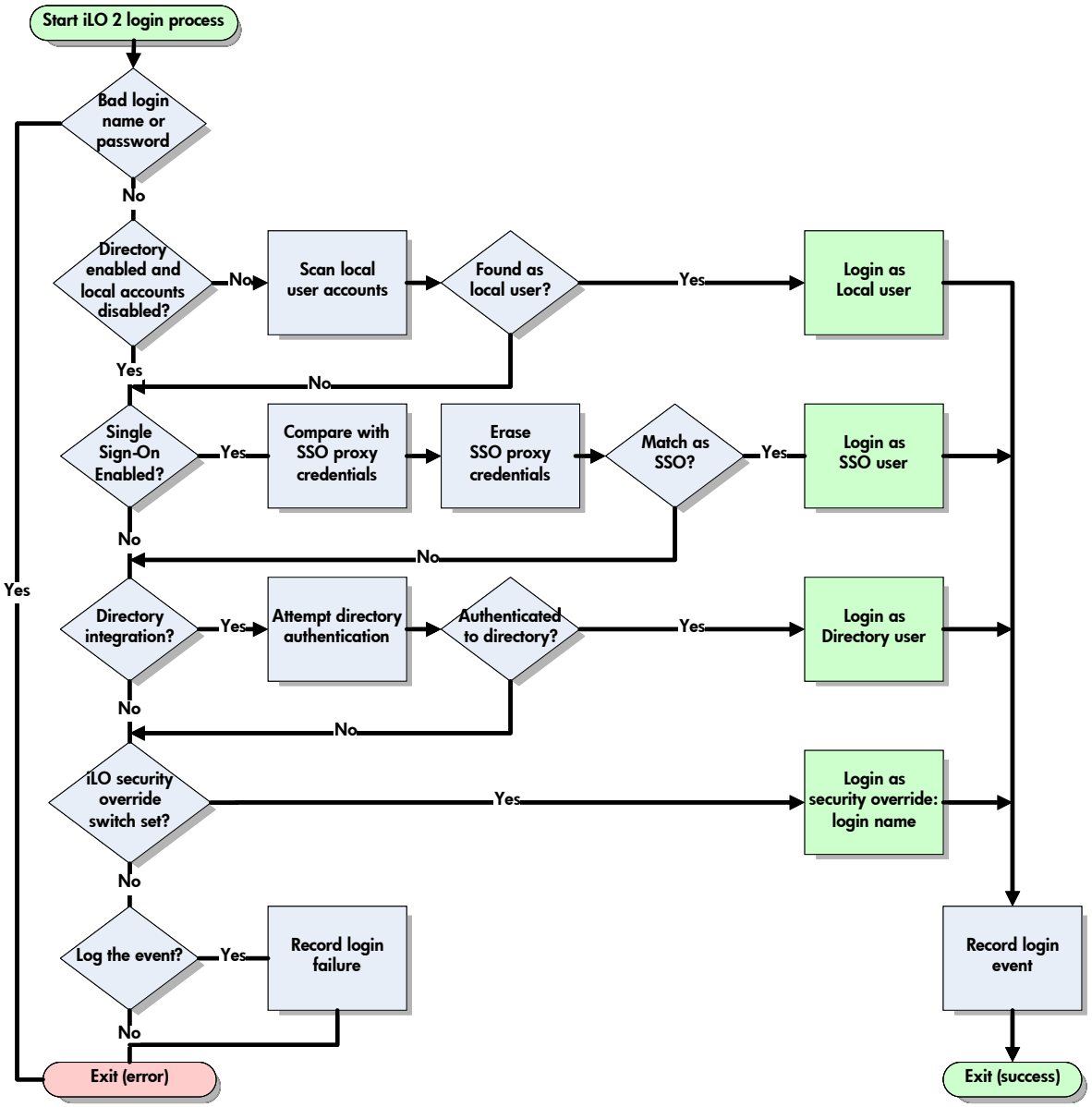
HTTP header line: Cookie hp-iLO-Login=00000007:QWRtaW5pc3RyYXRvcg=:Y29toGFx:
EUOHEFQUMYVZVYLQFDBSHJQJZUVVYTGQMOSZQGA

The cookie is stored in the memory of the client machine while you have the browser session open. Any open browser session may preserve a cookie, including a "spawned" browser session such as the remote console window. The client browser never writes the cookie to its disk drive. Only the client session that generated the cookie can access it. The browser destroys the cookie when you close the browser or log out of iLO. Therefore, you should close all browser instances to guarantee that the browser destroys the cookie.

After creating the cookie, the browser returns it to iLO with a request for a status page. iLO looks up the assigned user privileges through a generic login interface (API) to centralize the login functionality and to abstract the local and directory user accounts.

The common login API authenticates first against the directory, and then against local user accounts (Figure 5).

Figure 5. Flowchart of common login API that iLO performs using authenticated credentials in the cookie



After authenticating the user, iLO calculates the current privileges (see "Calculating current privileges") and sends the iLO Status Summary page to the client browser. The iLO Status Summary screen displays general information about iLO, such as all logged in users, server name and status, iLO IP address and name, and latest log entry data. The login process is then complete, and the user can perform any authorized functions.

Authentication and authorization with iLO 3

iLO 3 assigns to every authenticated session a unique and wholly random session cookie containing only the session key. To prevent redirected post and cross-site scripting attacks, the session key must be presented with every request and must be embedded in any request that makes changes to iLO 3 settings.

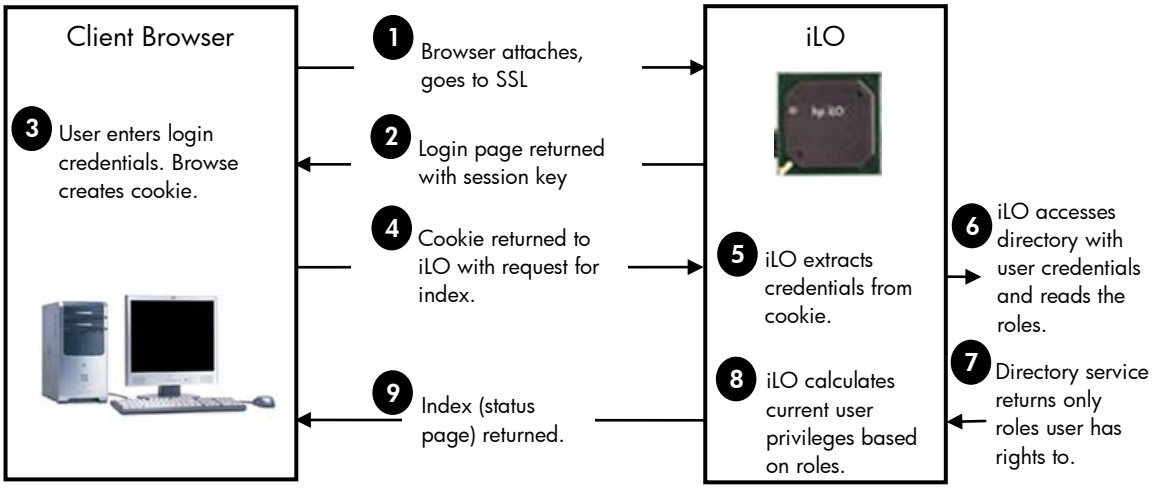
After authenticating the user, iLO calculates the current privileges and sends the iLO Status Summary page to the client browser. The login process is complete.

Login process using directory services with HP schema extensions

You can enable directory services to authenticate users and authorize user privileges for groups of iLO management processors. iLO directory services uses the industry-standard Lightweight Directory Access Protocol (LDAP/LDAPS). HP layers LDAP on top of SSL to transmit the directory services information securely to the directory servers.

Figure 6 shows the steps for the login process using directory services.

Figure 6. Login process when using directory services



Login process using directory services with HP default schema

You can also control access to iLO using the HP Default Schema method (sometimes referred to as Schema-free method). But you can use this *only* if you configure iLO with appropriate group names and their associated privileges. iLO acquires the user's name from the directory to determine group membership. iLO then cross-references the group names with its locally stored names to determine user privilege level.

The HP default schema login requires the user's full distinguished name to look up his or her group memberships. iLO cannot efficiently convert a username into the user's DN. iLO creates an IADsNameTranslate object and uses the Get method to retry the user's DN. If you enable ActiveX, the login script will call IADsNameTranslate to write the DN to a cookie. The login script gets the user's login credentials (user name and password), gets session information from iLO, and combines these into a security cookie. iLO uses this cookie to ensure that the user has access to the pages and resources he is trying to use.

Some IT organizations may prefer to disable ActiveX for security reasons. If you disable ActiveX in the browser or if the call fails and the name used for login is a DN, then the login script will work. The login script will also work if the name used is only a user object name. iLO combines the user object name with a user context to build a DN. The HP Default login process reverts to the login process for HP Schema if the IADsNameTranslate command is unavailable. See http://msdn2.microsoft.com/en-us/library/Aa706046.aspx for more information and examples.

NOTE

iLO 3 does not use ActiveX to do authentication and does not use the IADsNameTranslate control.

The username and password information in the cookie are enough for authentication and authorization using the local account database or using the directory with HP schema.

Using IADsNameTranslate lets you login using NetBIOS format (domain\username) or email format. See the previous Authentication and authorization sections with local accounts for information about using SSL, session keys, and cookies.

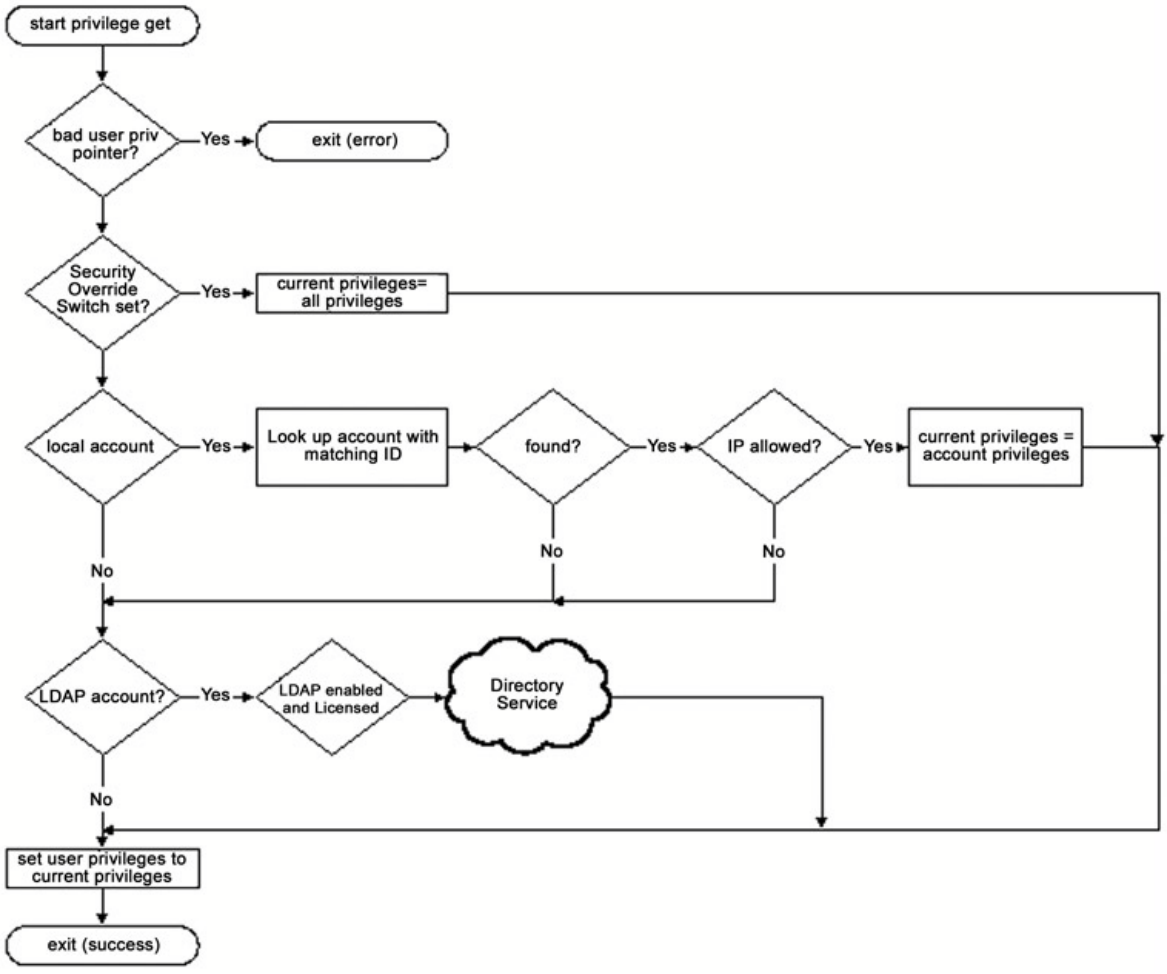
Calculating current privileges

A user's privileges can change at any time, even while the user is logged in:

- An administrator could change a user's rights while that user is logged into the iLO device and the browser session is open.
- A user might be authenticated with directory services but authorized to access the system only between 8 a.m. and 5 p.m.
- XML scripts could alter privileges.
- Administrators could delete a user account.
- Directory settings could change.
- Time or address-based restrictions could apply.

iLO re-evaluates a user's privileges every time he makes a request (Figure 7). iLO blocks the user's request or logs out the user if the evaluation fails.

Figure 7. Flowchart of iLO process for calculating current user privileges



Login process using two-factor authentication with Microsoft Internet Explorer (iLO 2 v1.80 only)

iLO 2 v1.80 provides an authentication scheme supporting only Microsoft® Internet Explorer. This authentication scheme involves using two factors of authentication:

- Something the user knows—a password or PIN.
- Something the user possesses—the private key for his digital certificate.

Users can store their digital certificates and private keys wherever they choose, such as on smart cards and USB keys.

When two-factor authentication is required, access to the OS on a remote server will use smart card device support within Windows Remote Desktop Connection. iLO uses Terminal Services pass-thru to access Remote Desktop Connection. Support for smart cards in Remote Desktop Connection requires that the remote server run Microsoft® Windows® Server 2003 or later.

The authentication layer will continue to be a middle layer between HTTP and LDAP or local accounts. The layer will provide certificate validation for local users, and perform the necessary LDAP calls to authenticate with the directory.

With two-factor authentication enabled for web browser access, access to the following ports is automatically disabled:

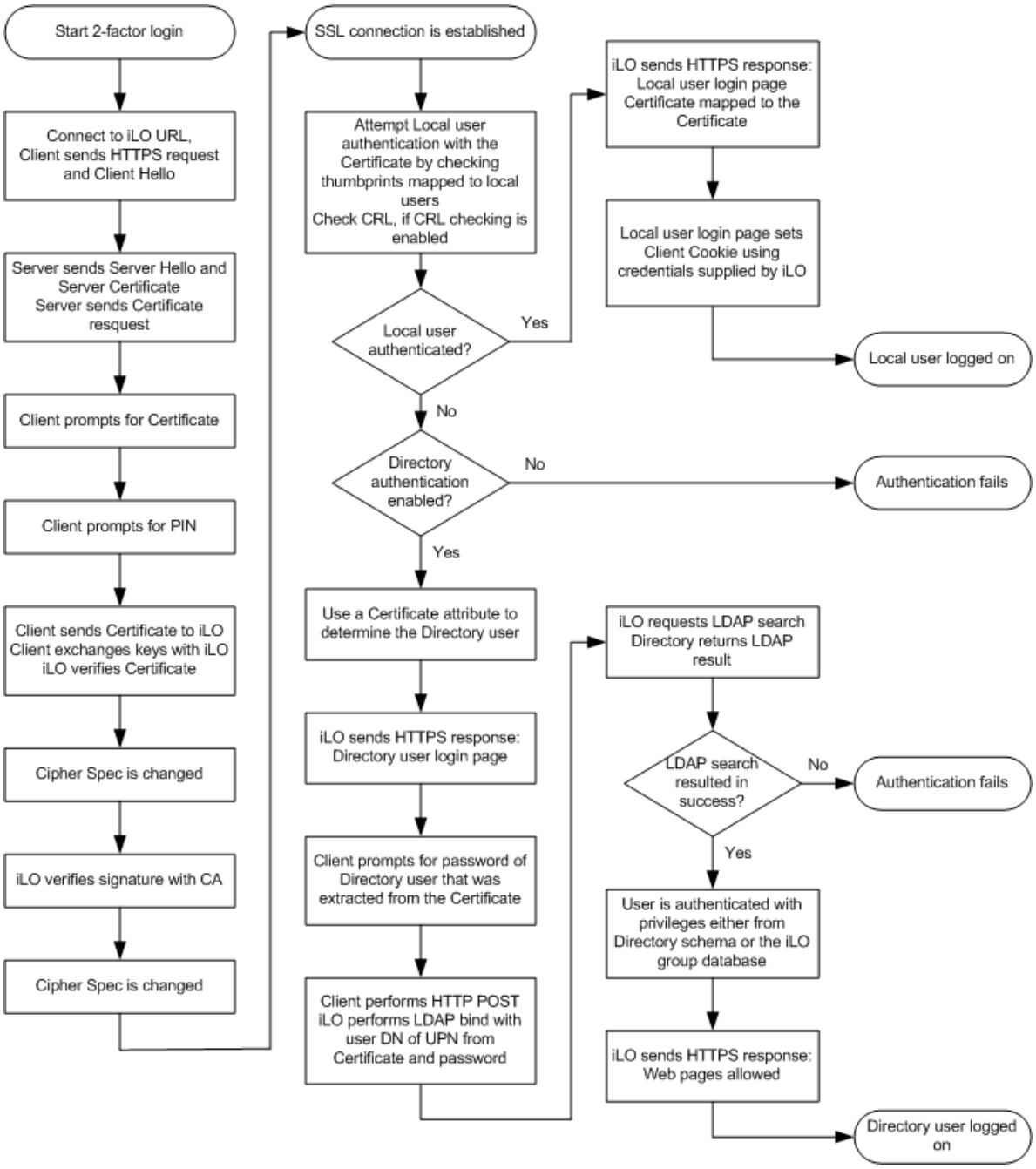
- SSH
- Port 22
- Telnet, Port 23
- SSL, Port 443 (XML traffic only; no other traffic is affected)

If necessary, server administrators can selectively re-enable the SSH and/or telnet ports manually. It is important to know that you cannot enable the XML port (CPQLOCFG access) while two-factor authentication is enabled. Performing group administration activities while you have two-factor authentication enabled requires using the HPONCFG utility.

Figure 8 shows the messages exchanged in two-factor mode to establish secure communication channels and authentication between the client and iLO, and between iLO and the directory.

The Microsoft Internet Explorer browser uses the Microsoft Cryptographic API for communication between the browser and the certificate contained in the smart card.

Figure 8. Two-factor authentication dialogue between the client and iLO, and between iLO and the directory server



Login process for remote console and virtual serial port with iLO and iLO 2

The iLO remote console server monitors the remote console port for connections from the remote console, virtual serial port applets, and possibly telnet. Initiating a remote console session involves the following steps (illustrated in Figure 9):

1. The user launches the Java applet by clicking on a link in the client browser.
2. The link opens a separate browser window.

3. iLO sends a secure one-time login token to the second browser window. The token contains base-64 encoded hash values of a random secret key and a random session key. iLO sends this token securely over SSL so a LAN sniffer cannot capture it.
4. The Java applet in the second browser window (using base-64) decodes the information within the token.
5. The Java applet passes the decoded information back to the remote console applet as the username and password.
6. The remote console applet compares the original login token with the decoded username and password from the Java applet, and allows a login if the data match.

This process is identical for the Integrated Remote Console ActiveX control.

Figure 9. Process for initiating a remote console session

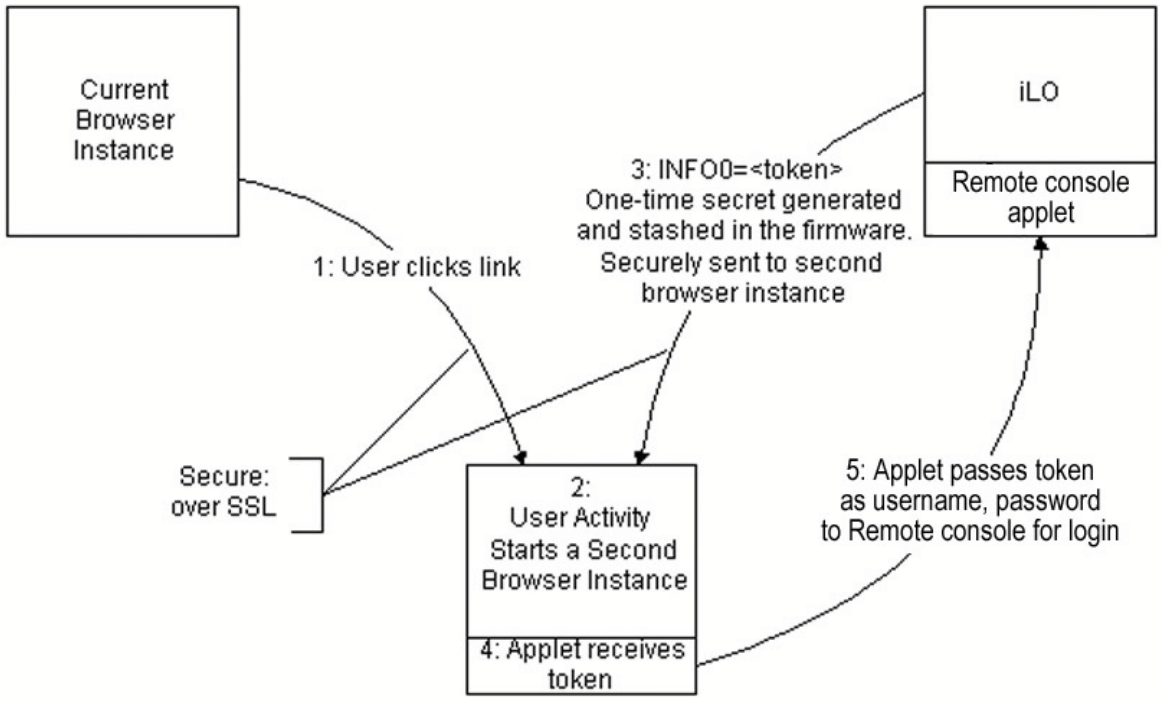
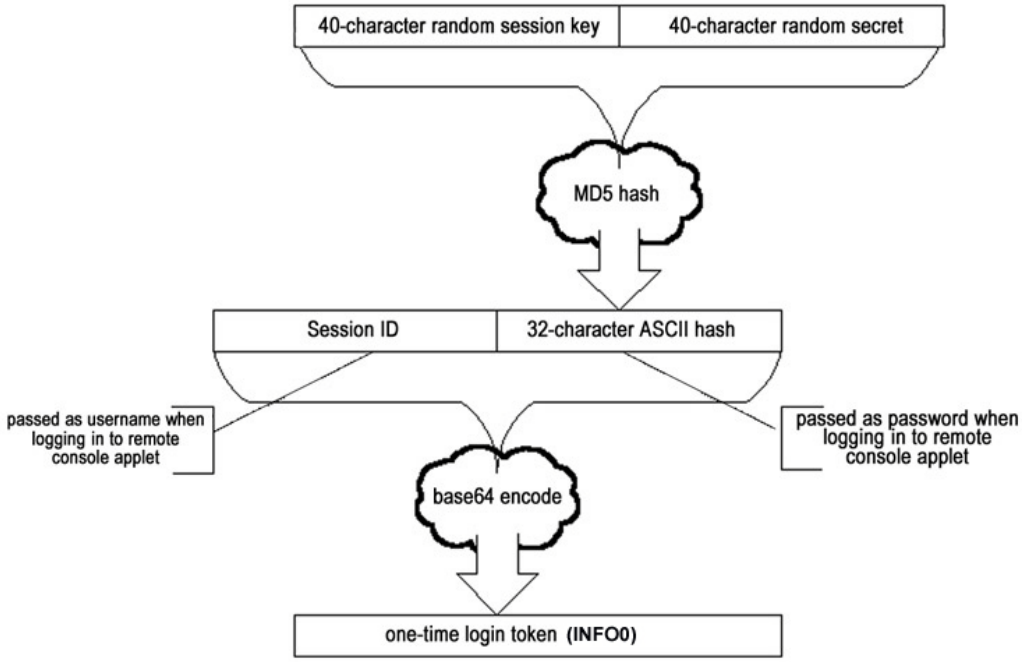


Figure 10 illustrates the steps required to construct the one-time login token for Java applet login:

1. The original browser session contains a 40-character random session key. Programming code stored in the remote console applet generates a 40-character random secret. The code concatenates the random session key with the random secret.
1. The iLO device performs an MD5 hash on the concatenated line, and then converts the MD5 hash to ASCII. An MD5 hash is a one-way encryption method that converts a message into a 32-digit hexadecimal number, also called a message digest. This step guarantees that the session key remains obscured and prevents a user from hijacking another session by using his valid session key to reattach to a different user's session.
2. The session ID is concatenated with the 32-character ASCII hash to obtain a second new line.
3. The result is base-64 encoded and sent to the applet.

Figure 10. Process that iLO uses to create the one-time login token for Java applet login



The result is that the applet passes the web server session ID as username and the ASCII hash as password to iLO. If iLO detects a match with the original 40-character random secret stored in firmware, iLO allows the login and matches the connection credentials with those stored in the session. Comparing the password with the stored secret destroys the secret. Successive attempts to connect using that 40-character secret will fail.

In addition to supporting the one-time secret login, the remote console applet supports traditional username and password login. With the remote console port configuration enabled and the remote console data encryption set to <no>, telnet can use the username and password credentials to connect iLO to the remote console port.

The new connection that the Java applet will use stays open as long as the server receives a "heartbeat" once every 30 seconds. The connection closes if the server does not receive a heartbeat within one minute.

iLO and iLO 2 support the Remote Console Computer Lock feature, which self-locks the operating system console when the session is closed or times out. Even though the session is closed, the connection remains active and authenticated to the OS. Without the Remote Console Computer Lock, another iLO user could access that open connection and start a new session. The console also self-locks if the network connection breaks during a remote session. Microsoft Windows and Linux® operating systems support this function. Server administrators can configure Remote Console Computer Lock using programmable RC hot-keys to let iLO users maintain a connection.

Login process for remote console and virtual serial port with iLO 3

iLO3 gives a second session key when you authenticate over HTTPs. The remote console application uses the second session key to authenticate to iLO 3 as indicated in Figure 9. Using a second session key does not require iLO 3 to perform an MD5 hash as described previously and shown in Figure 10. Note also that iLO 3 does not support telnet. Authentication with iLO 3 differs from authentication with iLO and iLO 2.

Single Sign-On

iLO v1.90, iLO 2 and iLO 3 support Systems Insight Manager (SIM) Single Sign-On (SSO). SIM SSO allows direct access to iLO through HP SIM without requiring an extra iLO login step. The user's HP SIM role determines the user's iLO rights. iLO 2 will trust SIM and users authenticated by SIM. The SIM SSO implementation uses a trusted certificate model for iLO to allow authentication to users from within the SIM framework.

Adding the BladeSystem Integrated Manager 2.4 or later provides SSO capability for iLO processors in server blades.

SIM SSO gives you the following capabilities:

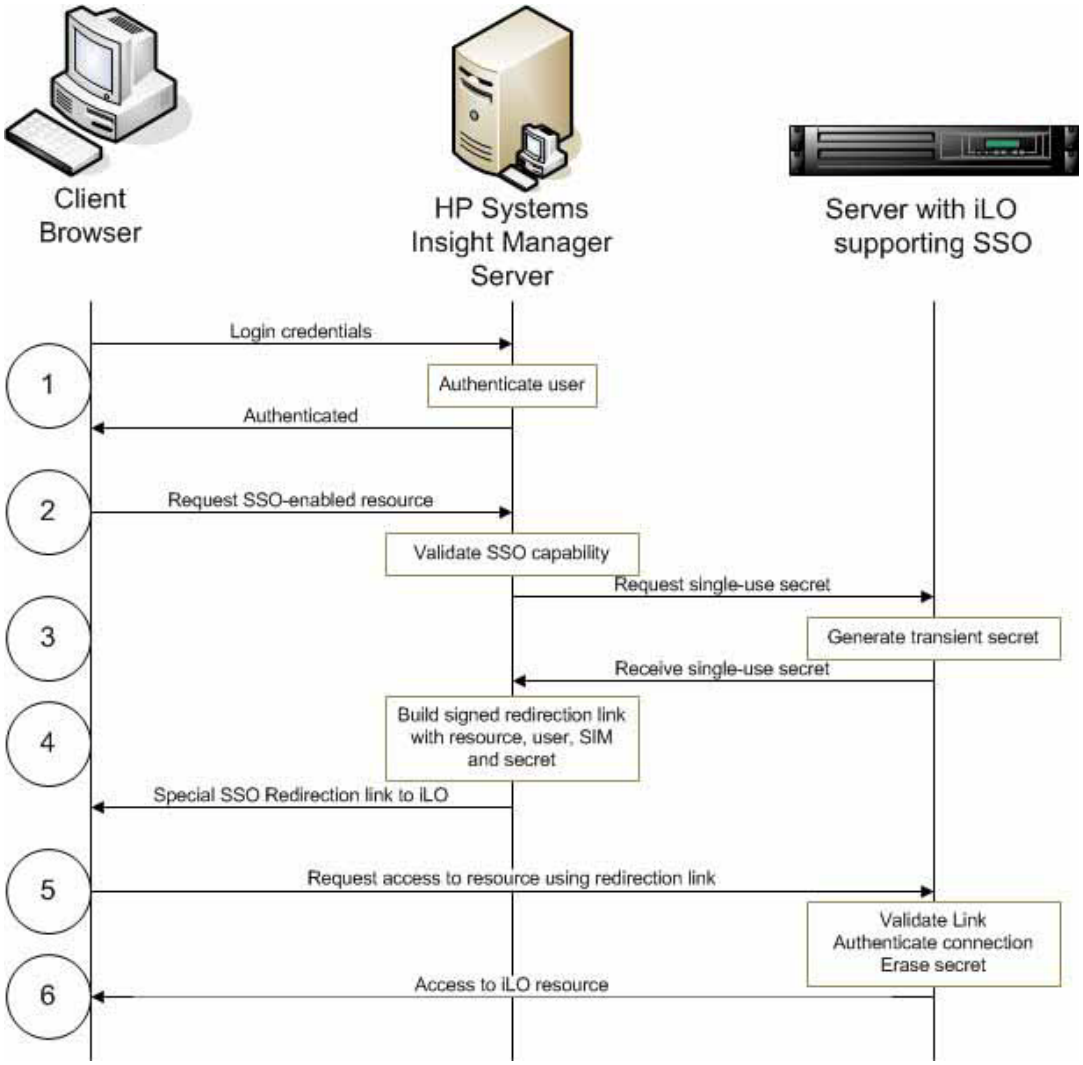
- Importing one or more SIM certificates
- Importing automatic certificate to ease initial setup
- Importing manual SSO certificate
- Mapping SIM role to user privilege
- Redirecting to the SIM console for SSO
- Modifying iLO login process to support automatic login from supported SIM SSO redirections

Figure 11 illustrates the authentication process from within the SIM framework:

1. The user logs-in to HP Systems Insight Manager Central Management Server.
2. The user follows a link in HP SIM. This link initiates the SSO connection.
3. iLO generates a timed, one-time secret to prevent replay attacks.
4. HP SIM builds a signed link including the resource, secret, user, and HP SIM.
5. Client browser redirects to the link at the iLO processor.
6. iLO validates the request based on the request contents, iLO configuration, secret, and HP SIM source. Authenticated requests receive the resource.

SIM SSO does not affect the local iLO user. SSO trust is iLO-based and iLO can determine the SSO status by server name, certificate, or both. HP recommends using certificates. Certificates must be imported to iLO. There is limited space to store certificates, so once the buffer fills, new records replace the oldest certificate data.

Figure 11. Process for HP SIM Single Sign-On to iLO



Authentication and authorization processes for CLI access

The iLO command-line interface (CLI) is an alternate method to access critical iLO functions such as the virtual power, text-based remote console, and virtual serial port. The iLO CLI uses the industry-standard SSH protocol to encrypt the data stream and all keystrokes sent between iLO and the client.

When a user requests an SSH session, the iLO processor performs the following negotiation steps to ensure a secure login:

1. The iLO processor retrieves the encryption keys from NVRAM. If the keys are not present or are invalid, the iLO processor generates the keys.

NOTE

Encryption keys are preloaded at the HP factory. However, for a field upgrade, creating the keys could take up to 25 minutes after upgrading the firmware. If users try to login through SSH immediately after upgrading, they could have to wait for up to 25

minutes. During this time, iLO response to other functionality is slow and the iLO status page displays a message indicating that key generation is in progress.

2. The iLO processor listens for a request on the SSH port. When it gets a request, it starts a protocol negotiation task for exchanging the public and private keys during the SSH protocol negotiation.
3. The protocol negotiation task completes the key exchange.
4. The protocol negotiation task then creates a task for checking authentication timeout and another task for performing the authentication. The authentication task also reads from the SSH port once authentication completes successfully.
5. The task for protocol negotiation then terminates while the authentication task and authentication timeout task continue to run.
6. The authentication timeout task waits for one minute. If authentication does not complete successfully during that time, iLO will terminate the connection.
7. The authentication task will attempt to authenticate the user. iLO allows a maximum of three attempts. If authentication is unsuccessful, iLO terminates the connection. If authentication is successful, the CLI session task for the SSH session and the SSH task for writing to the SSH socket will start. After initiating the CLI and SSH tasks, the authentication task becomes the read task for the SSH socket.
8. The write task for the SSH connection will write data to the socket. If there is no session activity for a period equal to the session timeout, the SSH session will close.

Authentication process for IPMI-Over-LAN access

The iLO 3 processor conforms to the Intelligent Platform Management Interface (IPMI) 2.0 specification for IPMI-over-LAN capability. This access method uses Remote Management Control Protocol (RMCP) that authenticates with a standard Message Authentication Code. For more information on the IPMI-over-LAN, consult the IPMI 2.0 Specification available at the IPMI website.

Encryption

The iLO management processor uses 128-bit SSL and SSH frameworks to ensure iLO privacy actions depending on the access modes and types of functions being performed. Within these frameworks, various ciphers can be used for encrypting network traffic.

The purpose of a cipher is to make data private so that only parties to the cipher and keys can read the data. The frameworks allow cipher negotiation and secure exchange of keys used to initiate encrypted communication within the cipher algorithm.

iLO supports RC4, 3DES, and AES ciphers for encrypting network traffic. Key exchange uses RSA/Diffie-Hellman, and keys are rotated every 3 minutes. Certificates are generated by iLO using 1024-bit RSA keys signed with MD5RSA and using a SHA1 fingerprint.

Secure sockets layer (SSL)

The iLO management processor encrypts all web pages using 128-bit SSL encryption. This ensures that all information and commands issued through the web browser are private. See "Authentication and authorization processes for browser access" for more information.

SSL allows the client (browser) and server (iLO) to compare a list of ciphers. Generally, they negotiate to use the strongest common cipher. A client may include a long list of ciphers, but iLO 2 v1.30 and iLO 3 can restrict the cipher list if desired.

AES encryption

iLO 2 v1.30 and iLO 3 can restrict ciphers to AES/3DES using browser settings (through the Global Settings page), XML scripting, or SM CLI.

The following is a complete list of communication operations that can employ AES encryption:

- Web browser (UI) – The current Mozilla browser, Firefox 2, supports AES Encryption. Internet Explorer 7 is the first Microsoft browser that supports AES encryption.
- LOCFG/XML –A command line switch that lets you select AES encryption and the cipher strength.
- SSH – You can initiate AES sessions with OpenSSH in Linux or PuTTY.
- LDAP– An outbound method of communication where iLO provides client-side communication and the LDAP server provides server-side communication.

The web browser, XML, and SSH support popular AES cipher strengths.

Remote console and virtual serial port data encryption

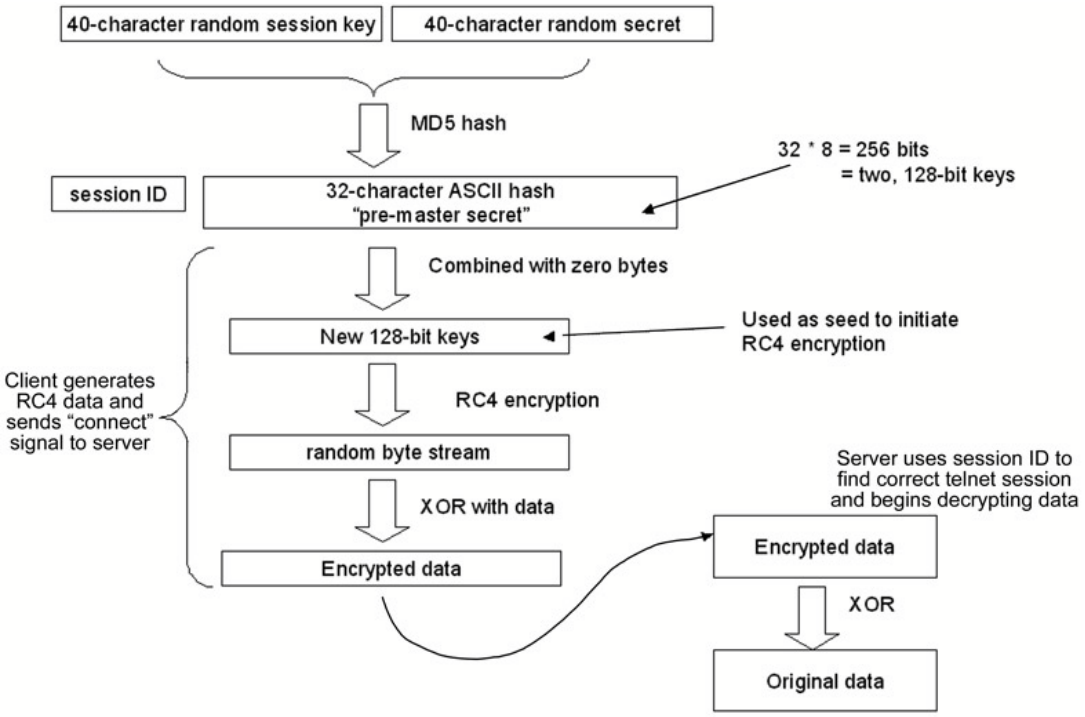
iLO uses the RC4 streaming cipher algorithm to encrypt remote console and virtual serial port sessions. Unlike a block cipher that encrypts several bytes of data at a time, a streaming cipher encrypts individual bytes, using a different key for each. For more information on RC4 and other encryption algorithms, visit the website at http://www.rsa.com/glossary/default.asp?id=1043 .

When a user requests either a remote console or a virtual serial port web page, iLO responds by using the MD5 hash algorithm to create a pair of random 128-bit keys (the "pre-master secrets") and a time-stamped session ID (Figure 12). These are the same session ID and MD5 hash values discussed in "Login process for remote console and virtual serial port." One key encrypts data from the client to the server; the other encrypts data from the server to the client. The time-stamped session ID is part of an array entry that identifies the telnet session. When the client browser tries to start an encrypted data session, it identifies itself with this session ID. The browser passes the128-bit keys and the session ID to the client using JavaScript files that ensure encryption of the security keys and IDs.

Next, the client generates the RC4 encryption data by combining the pre-master secrets with a set of zero bytes. This creates the new 128-bit keys used to initiate the RC4 encryption cipher. The client stores the new keys with the pre-master secrets in its dynamic memory space. The client does not write the keys to disk. The RC4 cipher algorithm generates a random stream of bytes and combines it with the remote console/VSP data in a Boolean XOR operation. This creates the encrypted data.

The client then sends the server a "connect" message containing a "start encryption now" signal and the session ID. After that, the client sends encrypted data. The server uses the session ID to find the correct telnet session and then begins decrypting the data using the RC4 cipher. The server performs another Boolean XOR operation on the encrypted data to recover the original data.

Figure 12. Remote console and virtual serial port encryption process



Every 3 minutes the server will combine the pre-master secrets with the generated 128-bit keys to create new 128-bit keys. It uses these new keys to create a new set of RC4 data. The server sends a signal to the client indicating that it has generated the new RC4 data and will begin communication using the new cipher. The client performs the same operation when it sees the signal. It then sends a signal to the server indicating that it is using the new RC4 data.

Secure Shell encryption

As discussed previously, the CLI uses SSH to encrypt the data stream both to and from the server. iLO encrypts the SSH data using either the 3DES-CBC or AES128-CBC protocols ("Appendix: SSH-2 support"). The SSH client negotiates with iLO to use one of those two protocols.

Disabling and changing ports

You can use iLO to change the port numbers of services or to disable services and utilities. You cannot reconfigure the SNMP ports. You can manually configure the numbers of these ports:

- HTTP port for the Web and XML server
- Telnet port
- Remote console port
- Terminal Services Pass-Thru port
- Virtual media port
- SSH port

For example, when given an IP address, a web browser normally attempts to connect with port 80. However, you can redirect the HTTP ports to administrator-defined ports. Once the HTTP port is re-directed, a user must specify that port and the IP address to access the iLO login screen. This reduces the chance that others can access the port without specific knowledge of the port number.

You can also selectively disable the services you do not need in your environment. Table 2 lists default port locations and indicates port status.

Table 2. Default port locations for iLO

Port No.	Protocol	Is Port Number Change allowed?	Supports	Enabled by default?
22 [1]	SSH	Yes	SSH Connections	Yes
23 [1, 2]	Telnet	Yes	• Remote graphical console • Remote text console • Virtual serial port	Yes
80	Remote Insight browser port	Yes	HTTP interface to iLO management board	Yes
161	SNMP get/set	No	HP SIM polls	No
162	SNMP trap	No	HP SIM agent events	No
443 [1]	Remote Insight browser access encrypted port	Yes	• SSL access to iLO management board • Encrypted XML access	Yes
623 [3]	IPMI over LAN	No		Yes
636	Lightweight Directory Assisted Protocol (LDAP)	Yes	Secure connection to the directory server	Yes, if directory support is enabled
3389 [2]	Terminal Services Pass-Through	Yes	Terminal Services session- software-based remote console using Microsoft Windows (RDC/TS)	Yes
9300 [2]	Telnet	Yes	Multi-user remote console	No
17988	Virtual Media	Yes	Virtual Media	Yes
17990	Telnet/ Remote Console [4]	Yes	Console replay	No

[1] Port disabled if two-factor authentication is enabled for web browser access.
[2] Not used by iLO 3.
[3] iLO 3 only.
[4] iLO 3 uses only Remote Console protocol.

Connectivity between iLO, the server, and the network

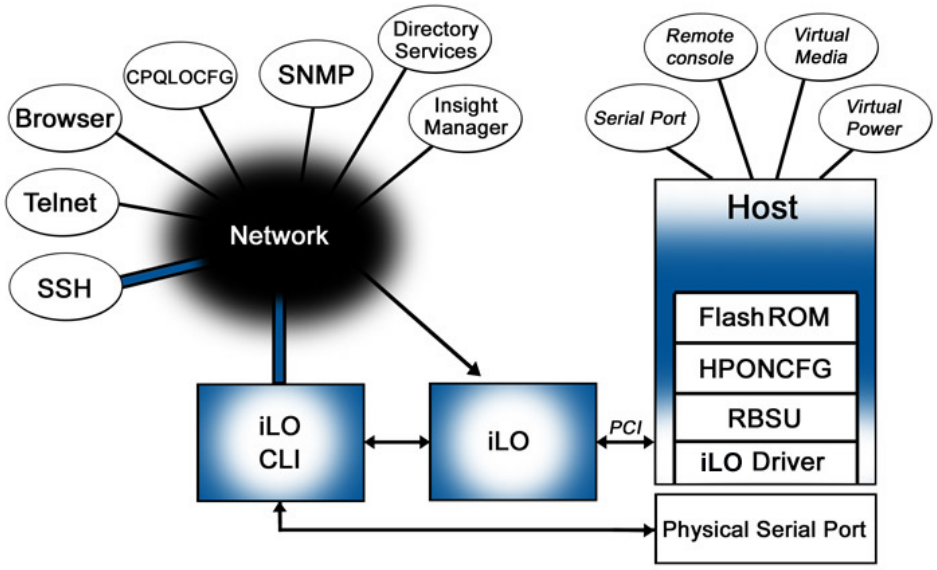
Knowing the points of access to and from iLO, the server, and the client helps you understand the potential for security risks. The following sections briefly describe how the iLO design or its configuration mitigates those risks.

Network access to iLO

These utilities identified in Figure 13 have access to the iLO processor through the network: SSH connection, telnet connection (except for iLO 3), the web browser, the CPQLOCFG utility, SNMP, directory services, the Lights-Out Migration Utility (for directory services), and Systems Insight Manager or Insight Manager 7. CPQLOCFG is a Windows-based utility that allows users to configure iLO devices. It sends RIBCL (XML) script files to iLO using a secure connection over the network.

We recommend that you keep iLO management traffic on a separate management network and grant access only to administrators. This improves performance by reducing the traffic load across the main network and defends against security attacks.

Figure 13. Linkages of the iLO processor to the network and host server



NOTE: iLO 3 does not use telnet.

Web browser

The browser encrypts the data stream using 128-bit SSL to provide privacy and integrity. iLO accepts digital certificates, so users can import certificates from a guaranteed certificate authority to prevent anyone from placing a Trojan horse server on the network. Administrators can change the default port location for the web browser. Finally, user access privileges and the strong authentication process restrict access to iLO through the web browser.

Telnet, remote console, and virtual serial port (iLO v1.30 and iLO 2 only)

Because telnet is not an inherently secure protocol, administrators may be reluctant to use it. This section describes iLO support for secure telnet access. The remote console and virtual serial port functions use the standard telnet port to connect to iLO. Although telnet itself is not encrypted, invoking the remote console applet enables encryption. This forces iLO to connect using the remote console applet rather than a standard telnet session for a text-based console session. iLO maintains exclusive control over the port.

You can configure the telnet port to allow only the remote console and virtual serial port functions—the "automatic" setting for port 23. This means that iLO disables the port except when it senses the remote console or virtual serial port applets starting. iLO refuses any other connection attempt to port 23, so the server will be inaccessible through a standard telnet application.

A standard telnet application can connect to the server in two ways. The first occurs after the user clicks on the remote console or virtual serial port but before the applet connects to iLO. If you enable encryption, iLO will close the connection as soon as it realizes the client has not sent valid information to begin the encrypted communication. The second way is if a client terminates abnormally: iLO will not close the socket until it realizes that no keep-alive signal has arrived during the specified one-minute interval.

You can change the telnet port number to any unused port number or disable the telnet port entirely. When the remote console port is in the "Disabled" mode, no application can connect to port 23.

Finally, the strong authentication and authorization processes of the remote console and virtual serial port applets reduce any potential security risk for telnet port across the network.

Multi-user Integrated Remote Console

iLO v1.90, iLO 2 v1.30, and iLO 3 offer IRC as an iLO Advanced and iLO Select feature. The IRC is a user-configurable setting that supports up to four simultaneous remote console sessions on the same server.

The first user to initiate a remote console session becomes the session host. The session host can deny access, grant full access, or allow read only access. Participant sessions end when the host session ends. iLO encrypts all console sessions. For added security, the Remote Console Computer Lock feature can self-lock the operating system when the session closes or times out.

Windows and Linux operating systems support IRC. The client browser on the management console must use a Windows Internet Explorer browser because the IRC uses the ActiveX code, not Java.

SSH for the command-line interface

Administrators with access to the CLI can access most iLO functions; however, they access iLO in text mode rather than in graphical mode. To ensure data and keystroke integrity, the SSH data stream is encrypted. Administrators can disable the SSH/CLI functionality, change the SSH port number, or restrict user privileges to ensure that only authorized persons can access the CLI.

CPQLOCFG utility

The CPQLOCFG utility connects to the iLO processor across the network using the encrypted SSL port. Users can only access the CPQLOCFG utility with valid user credentials and privileges authorized by the strong iLO authorization process. Administrators can change the HTTPS port number to reduce the likelihood of unauthorized persons accessing iLO.

Directory services

iLO uses SSL-protected LDAP to communicate with the directory server. Using directory services is more secure than using local iLO user accounts for these reasons:

- It eliminates the practice of sharing administrator accounts among multiple people.
- The directory enforces password protection.
- Role-based access allows access restriction by detailed time and place.
- You can perform maintenance functions (such as changing rights for multiple users) once at the directory rather than once for each iLO device.

Administrators using the Lights-Out migration utility to migrate from local accounts to directory accounts access iLO through the network. HP built the Lights-Out migration utility on top of the XML infrastructure of CPQLOCFG, so it has the same security advantages as CPQLOCFG: strong authentication, ability to change port numbers, and encryption.

SNMP

iLO acts strictly as a pass-thru service for SNMP functions. The SNMP port is one of only two ports in iLO that pass traffic to the OS through the iLO driver. Remember that SNMP does not encrypt data. You can disable SNMP if you are concerned about data that iLO passes from the server, such as the OS, type of processor, and number of I/O devices. If you want to use SNMP, you can set firewalls and routers to accept only specific source and destination addresses. You can also set passwords (community strings) according to the same guidelines as administrative passwords.

HP Systems Insight Manager

HP SIM checks for an iLO presence by starting an HTTP session. Tight integration between iLO and SIM means that you can use HP Insight Management software to get server serial numbers, iLO status and serial numbers, and hardware/firmware revision data.

Physical access to iLO

Someone physically present at the server can access iLO in one of two ways:

- Through the physical serial port on the server
- By means of the iLO Security Override jumper

Server serial port

Users with access to the server serial port can access the iLO CLI and perform many iLO functions on the server. A potential risk is that the connection from the serial port to the CLI is not encrypted. However, we assume that anyone with physical access is authorized to access iLO. Because the server serial port connects to the iLO CLI, you can disable the SSH/CLI functionality or restrict user access by requiring authentication to the CLI. You can also change the server OS to disable any support for the server serial port.

iLO Security Override jumper switch

People with physical access to a server can alter the server and the iLO setup. They can access the security override jumper, reconfigure iLO through RBSU, reprogram the iLO ROM, or reprogram the boot block. Therefore, data center managers must ensure that only super-users or administrators have unrestricted access to the inside of a server enclosure. Consult the server documentation for the location of the iLO Security Override jumper.

Access to the server from iLO

You can directly access the server through iLO functions such as virtual serial port, remote console, virtual media, and Terminal Services (Figure 13). iLO secures the environment through strong user authentication and authorization processes.

iLO software on server using the PCI bus

Several pieces of iLO software reside on the server and provide an entry point into the server. The iLO driver enables the other iLO integration services, such as RBSU, Terminal Services pass-thru, HPONCFG, and the agents.

RBSU

RBSU lets you initially configure iLO and iLO user accounts. RBSU is available to anyone with access to the server console when the server boots. You can configure RBSU to require valid user credentials using the robust iLO login mechanisms. If you don't want RBSU to be accessible at reboot, you can disable RBSU in the Global Settings preferences. Disabling RBSU prevents reconfiguration from the server unless the iLO Security Override Switch is set.

iLO firmware (FlashROM)

The ROM boot block protects the iLO firmware by using a digital signature created with a private key known only to HP. The iLO boot block verifies the digital signature by using a corresponding public key. No one can modify the firmware contents without generating a new digital signature. This requires the original private key from HP. The boot block examines the digital signature of the iLO main-line code and refuses to transfer control to the main-line code if the signature is invalid. This prevents loading corrupt or rogue firmware.

HPONCFG

The HPONCFG utility is a server-based service that can configure iLO using XML scripts. Because it is server-based, the iLO firmware ignores login credentials and assumes that the user has the rights to configure iLO. HPONCFG reduces this potential security risk by requiring a root login in Linux operating systems or administrator login in Windows operating systems to access the utility.

CPQLODOS

You can use the CPQLODOS utility for initial iLO processor deployment, but only locally in a DOS environment such as during a SmartStart scripted deployment. The administrator must have a DOS image loaded on a server or a floppy. This means that the user has either physical access or a virtual media privilege, with all the accompanying user rights and authentications.

Terminal services

iLO uses the pass-thru service HPLOPTS.EXE to access Windows Terminal Services. The iLO remote console applet activates the Terminal Services client application when you request a remote console connection. iLO sets up a socket and monitors port 3389. The iLO processor passes thru to the server all data that it receives from the Terminal Services client and vice-versa. iLO implements security identically to the Windows Terminal Services Remote Desktop Protocol implementation. This means that any active security measures are established between the Microsoft terminal services client and the Microsoft Remote Desktop Protocol service.

The Terminal Services port is the second of two ports in iLO that allow traffic to pass to the OS through the iLO driver. Administrators can disable the Terminal Services pass-thru port.

IT infrastructure security considerations

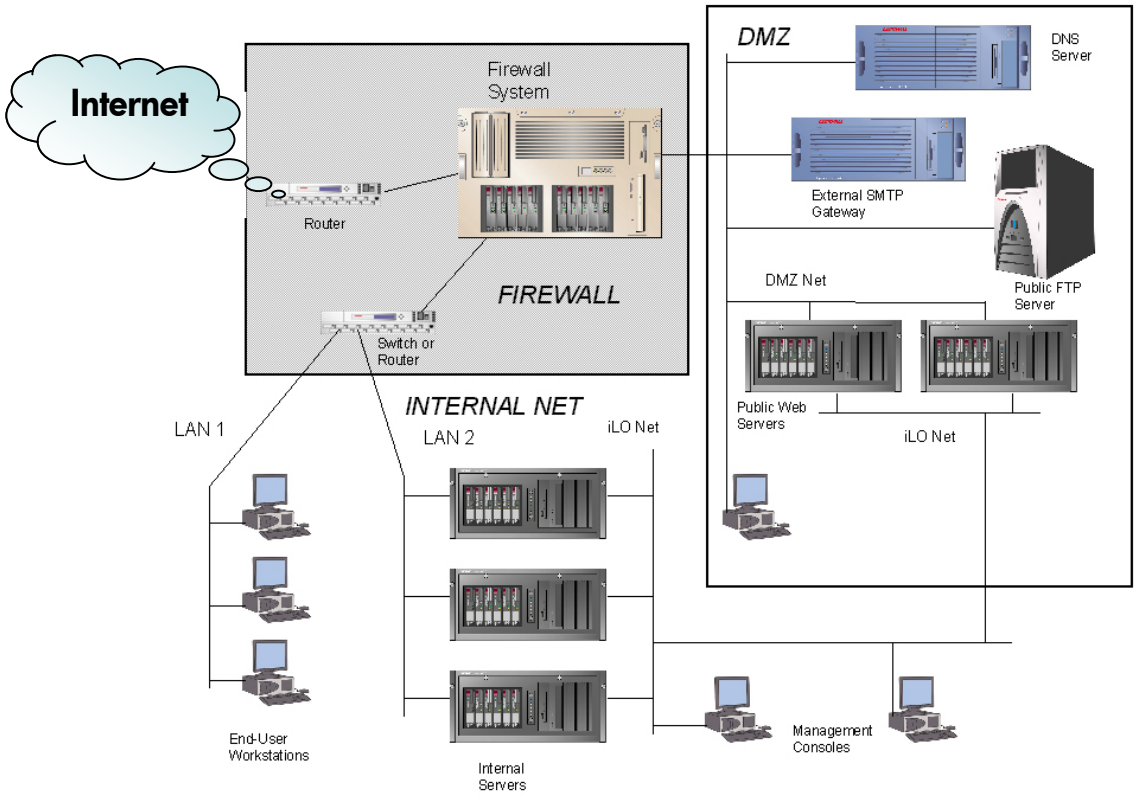
The following sections describe iLO security in two particular IT environments:

- When operating in the infrastructure between an external firewall and an internal network (DMZ)
- When operating in a server blade environment

Operating iLO servers in the DMZ

An Internet-connected architecture typically has a more secure, de-militarized zone (DMZ). The DMZ zone lies between the corporate servers and the Internet. It usually has firewalls that restrict traffic flow between the corporate/Internet areas. This architecture lets you access servers that provide publicly available Internet services through a firewall, but you cannot access these services on the internal network. This more secure zone provides an area isolated from the internal network and hardened against external attack (Figure 14). The security challenges in the DMZ require a careful balance between critical security requirements and the need to effectively manage and maintain the systems.

Figure 14. Example configuration of a DMZ



iLO can create a separate, secondary network (iLO Net in Figure 14) parallel to the primary or production network. This dual-network architecture segregates management traffic from production network traffic. It allows system-wide server management activities, including servers inside the DMZ, while maintaining maximum security by limiting access to the production network.

Figure 14 shows a packet-filtering router that acts as an initial line of defense. Behind this router is a firewall system. There is no direct connection from the Internet or the external router to the internal network. All traffic to or from the internal network must pass through the firewall system. An additional router filters packets destined for the public services in the DMZ and protects the internal network from public access.

The firewall is a multi-targeted server that you can configure to evaluate traffic according to different rules based on the traffic source and destination:

- From the Internet to the DMZ
- From the DMZ to the Internet
- From the Internet to the internal network
- From the internal network to the internet
- From the DMZ to the internal network
- From the internal network to the DMZ

Servers inside the DMZ and on the internal network can use iLO processors. There is no possibility for data to flow between the DMZ network and the iLO network because the network connection to iLO is

completely isolated from the network ports on the server. Even if the DMZ network were compromised, the iLO network would remain secure. This lets you use iLO on servers located in the DMZ or in the internal network without compromising sensitive data. Administrators create this separation by using a dedicated NIC or the SNP with its VLAN (see the section "SNP for select ProLiant servers").

For best protection of the servers operating inside the DMZ, set the SNMP trap destinations to the loop back address and enable the SNMP pass-thru in iLO to route traps onto the iLO network. This SNMP pass-thru option does not activate all management functions. However, it does pass status, inventory, and fault information to HP SIM or another SNMP-capable management application. This option is very secure because the OS does not recognize the iLO product as a NIC.

The Rapid Deployment Pack Deployment Server Console provides secure access to the management functions of iLO and Remote Insight Lights-Out Edition (RILOE).

HP Rapid Deployment Pack combines an off-the shelf version of Altiris eXpress Deployment Solution and the ProLiant Integration Module. The ProLiant Integration Module includes:

- SmartStart Scripting Toolkit
- Configuration Events for industry-standard OSes
- Sample unattended files
- ProLiant Support Packs containing software drivers and management agents

Administrators can deploy servers through the Altiris' imaging feature or through scripting using the SmartStart Scripting Toolkit. HP Rapid Deployment Pack is a part of HP Insight Control Management Software. See the HP website for more information about HP Insight Control Management Software.

Communication between iLO and server blades

The HP BladeSystem architecture uses a single enclosure to hold multiple servers. A separate power subsystem provides power to all servers in that enclosure. ProLiant c-Class server blades use iLO to send alerts and management information throughout the server blade infrastructure.

There is a strict communication hierarchy among ProLiant c-Class server components. The Onboard Administrator (OA) management module communicates with the iLO processor on each server blade. The OA module provides independent IP addresses for each server blade. The iLO device on a server blade also maintains an independent IP address. The iLO firmware exclusively controls any communication from iLO to the OA module. There is no path from an iLO processor on one server blade to the iLO processor on another blade. There is no connection from the iLO processor or OA module to the server NICs. The iLO processor only has information about the presence of other server blades in the infrastructure and whether enough amperage is available from the power subsystem to boot the iLO server blade. A single, physical port on the rear of the BladeSystem enclosure provides access to the iLO network connections on the server blade. This simplifies and reduces cabling.

Security audits

Recent legislation may mandate periodic security audits. iLO maintains an event log containing date- and time-stamped information pertaining to events that occurred in the iLO configuration and operation. You can manually access this log through the System Status tab of the iLO browser interface. You can also use XML commands to set up an automated examination and extraction process that parses the event log by date/time and by authenticated user for accessing information about security events.

General security recommendations

We recommend that you observe the following security practices:

- **Use a separate management network.** We recommend that you establish a private management network separate from your data network and that only administrators have access to that management network.
- **Do not connect iLO directly to the Internet.** The iLO processor is a management and administration tool, not an Internet gateway. Connect to the Internet using a corporate VPN that provides firewall protection.
- **Change passwords frequently if using local accounts.** Change the default iLO password immediately to a more relevant password. Administrators should change the iLO management passwords with the same frequency and according to the same guidelines as the server administrative passwords. Passwords should include at least three of these four character types; numeric, special, lowercase, and uppercase
- **Implement directory services.** This allows authentication and authorization using the same login process throughout the network. It provides a way to control multiple iLO devices simultaneously. Directories provide role-based access to iLO with very specific roles and privileges based on time and location.
- **Implement two-factor authentication.** This provides additional security, especially when you can make connections remotely or outside the local network.
- **Restrict access to remote console port**. Restrict access to the remote console port and turn on encryption to provide tighter security. We recommend disabling the port entirely if you don't require the remote console.
- **Protect SNMP traffic**. Reset the community strings according to the same guidelines as the administrative passwords. Also set firewalls or routers to accept only specific source and destination addresses. Disable SNMP at the server if you don't need it. You can also disable the iLO SNMP pass-thru.

Conclusion

iLO lets you deploy your ProLiant servers without concern. It uses strong authentication, highly configurable user privileges with strong authorization processes, and encryption of data, keystrokes, and security keys. The hardware design protects keys and sensitive password information. It also lets you separate iLO management traffic from all server traffic.

A networked environment has inherent security risks. iLO mitigates many of these risks through authorization, authentication, and encryption. You can further decrease the chance of attacks by following security recommendations, being aware of access points to the iLO devices and their servers, and configuring their networks to eliminate unnecessary services.

Appendix: SSH-2 support

Table A-1. SSH features that iLO supports

	SSH-2 Standard	iLO 2 SSH	iLO 3 SSH
Encryption (same set supported both ways)			
3des-cbc	Required	Supported	Supported
blowfish-cbc	Recommended	Not supported	Not supported
twofish256-cbc	Optional	Not supported	Not supported
twofish192-cbc	Optional	Not supported	Not supported
twofish128-cbc	Recommended	Not supported	Not supported
aes256-cbc	Optional	Not supported	Supported
aes192-cbc	Optional	Not supported	Supported
aes128-cbc	Recommended	Supported	Supported
serpent256-cbc	Optional	Not supported	Not supported
serpent192-cbc	Optional	Not supported	Not supported
serpent128-cbc	Optional	Not supported	Not supported
Arcfour	Optional	Not supported	Not supported
idea-cbc	Optional	Not supported	Not supported
cast128-cbc	Optional	Not supported	Not supported
None	Optional, but not recommended	Not supported	Not supported
Hashing algorithm			
Hmac-sha1	Required	Supported	Supported
Hmac-sha1-96	Recommended	Not supported	Not supported
Hmac-md5	Optional	Supported	Not supported
Hmac-md5-96	Optional	Not supported	Not supported
None	Optional	Not supported	Not supported
Compression			
Zlib	Optional	Not supported	Not supported
None	Required	Supported	Supported
Language			
English (same as current Telnet)		Supported	Supported
Key exchange			
Diffe-Hellman-group1-sha1	Required	Supported	Supported
Public Key algorithms			
ssh-dss	Required	Supported	Supported
ssh-rsa	Recommended	Supported	Not supported
X509v3-sign-rsa (certificates)	Optional	Not supported	Not supported
X509v3-sign-dss (certificates)	Optional	Not supported	Not supported
Spki-sign-rsa (certificates)	Optional	Not supported	Not supported

Table A-1. SSH features that iLO supports

	SSH-2 Standard	iLO 2 SSH	iLO 3 SSH
Spki-sign-dss (certificates)	Optional	Not supported	Not supported
Pgp-sign-rsa (certificates)	Optional	Not supported	Not supported
Pgp-sign-dss (certificates)	Optional	Not supported	Not supported
Client/User Authentication Method			
None	Must not be listed		
Public key	Required	Not supported	Supported
Server based	Optional	Not supported	Not Supported
Password		Supported	Supported
Client/User authentication parameters			
Default authentication timeout	10 minutes recommended	Hardcoded to 1 minute	Hardcoded to 10 minutes
Default SSH port	Default 22	Configurable. Defaults to 22.	Configurable. Defaults to 22.
Default number of attempts	20 recommended	Hardcoded to 3	Hardcoded to 3
User initiated key generation		Not supported	Not supported

For more information

Resource description	Web address
Integrated Lights-Out home page	www.hp.com/go/ilo
Industry-standard servers technology papers	www.hp.com/servers/technology
Integrated Lights-Out Documentation Includes links to the Planning and configuration recommendations for Integrated Lights-Out processors, Integrated Lights-Out user guide, and other documents related to iLO	http://h18004.www1.hp.com/products/servers/management/ilo/documentation.html
Directory support on Lights-Out management products	http://h18004.www1.hp.com/products/servers/management/directorysupp/index.html
Software and drivers for Lights-Out processors	www.hp.com/go/ilo
Lights-Out supported servers	www.hp.com/servers/ilo/supportedservers
Information about iLO 2 Advanced licenses	www.hp.com/servers/iloadv2
Information about IPMI and IPMI 2.0 specification	http://www.intel.com/design/servers/ipmi/

Call to action

Send comments about this paper to TechCom@HP.com

TC101208TB, December 2010